What is the Random Data method?

The Random Data method is a software-based Data Sanitization method, used in some file shredder and data shredder programs to overwrite existing information on hard drives or other storage devices.

The Random Data method, sometimes called the Random Number, is a software-based Data Sanitization method, used in some file shredder and data destruction programs to overwrite existing information on a hard drive or other device. other host.

Erasing your hard drive with the Random Data method will prevent all software-based file recovery methods from finding the information on the drive, and can also prevent most hardware-based recovery methods from extracting information. .

Keep reading the following article to learn how the Random Data method works and a few examples of programs that support the Data Sanitization method.

How does the Random Data method work?

Some Data Sanitization methods override existing data with zeroes or zeroes, such as Secure Erase or Write Zero. Other methods include both 0 and 1, but also have random characters, such as the Schneier method, NCSC-TG-025 and AFSSI-5020. However, the Random Data method, as its name suggests, uses only random characters.

This Random Data method is implemented in many different ways:

1. Override a random character 1 -? little by little

Tip : The Data Sanitization NZSIT 402 method is very similar to Random Data. It also writes random characters but includes a verification step at the end of the overwriting process.

Most data destruction tools that provide Random Data use it as a DIY method, allowing users to customize the number of overrides. Therefore, you may find this method of data deletion run at least 2 times or at most 20 or 30 times or more. You also have the option of verification after each or only the last override.

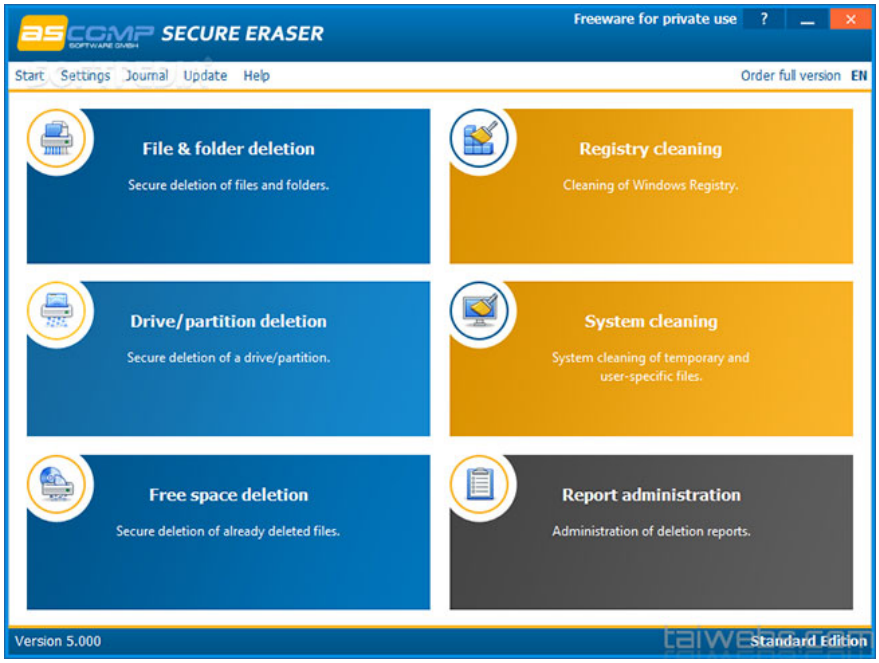
When a program runs verification after overwriting, it means that it verifies that the data was actually overwritten, in the case of this method, by random characters. If verification fails, the program uses the Random Data method that will prompt you to run the task again, or it will automatically overwrite the data.

Note : Some data shredder and file shredder programs allow you to customize not only the number of overwrites, but also the characters used. For example, you can choose the Random Data method, but then are given the option to override the number by 0.

However, although the program may allow you to customize the Data Sanitization method, everything that goes too far beyond what is explained above will result in a method that is no longer a random data.

The program supports Random Data

Many data shredders and file shredders support the Random Data method. Some programs that allow you to erase an entire hard drive using the Random Data method include DBAN, Macrorit Disk Partition Wiper, Eraser and Disk Wipe. Another option is CBL Data Shredder, but you must create your own template because the Random Data method is not included by default.



The file shredder program allows you to delete specific files and folders but not the entire storage device at once. Freeraser, WipeFile, Secure Eraser, TweakNow SecureDelete and Free File Shredder are just a few examples of file shredders that support the Random Data method.

Most data destruction programs support a variety of data sanitization methods, in addition to random data. For example, you can open any of the above programs and choose to use a different Data Sanitization method if you later decide to try another option.